National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Digital Policy Management Capability

Version 1.1.1

Digital Policy Management consists of a set of computer programs used to generate, convert, deconflict, validate, assess effectiveness, provide for distribution and deployment, and execute machine-readable policies used to enforce how resources are managed, used, and protected.

07/30/2012

CGS Digital Policy Management Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Digital Policy Management consists of a set of computer programs used to generate, convert, deconflict, validate, assess effectiveness, provide for distribution and deployment, and execute machine-readable policies used to enforce how resources are managed, used, and protected. These policies may include rules for authentication (e.g., trusted authorities, criteria for determining authenticity), system configurations, access rules, authorized sources of record or sources of reference, transport connectivity, bandwidth allocation and priority, audit event collection, and computer network defense monitoring and response (e.g., course of action).

The Digital Policy Management Capability refers to digital policy as expressed in machine-executable form so that it can be directly implemented in systems without human intervention. Non-digital policy is policy that is encapsulated in human language (even if the policy is captured in a “digital form”). Non-digital policy is covered in the IA Policies, Procedures, and Standards Capability.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Digital Policy is policy that can be encoded in a digital form, distributed, installed, and continuously checked for compliance without human intervention. Digital Policy Management provides a set of standardized and automated activities that are required to generate, convert, deconflict, validate, assess effectiveness, provide for distribution and deployment, and execute machine-readable policies throughout an Enterprise.

The Digital Policy Management Capability shall be able to generate and manage both globally and locally applicable policy, respond rapidly to changing conditions and to new mission requirements, scale to accommodate the global scope of a federated Enterprise, and operate effectively in both strategic and tactical environments. The Digital Policy Management Capability shall be flexible enough to adjust policies in real-time (or as close to real-time as possible) to respond to changing needs.

Generation of digital policies encompasses the creation of digital policies specific to defined endpoints. These digital polices are created based on organizational policies, which are in compliance with higher policies, provided by authoritative sources (e.g., source of record, source of reference).

The Digital Policy Management Capability shall be responsible for converting between many different types of policies (business rules/doctrine) and digital policies from high level to executable. Conversion of digital policies shall automatically translate the policy into a standard format executable by the applicable device, such as conversion between network devices. Automatic conversion may not be available for all devices but shall be used where possible.

The Digital Policy Management Capability includes deconfliction, which analyzes single or multiple policies to determine if they are consistent and contain no internal contradictions within the policies or between policies. An administrator shall manually decide the correct policy/policy statement to follow to implement in the Enterprise.

The Digital Policy Management Capability shall include validation to determine the impacts of new digital policies. Analysis that tests new or modified policies for adverse conditions prior to implementation in the environment is necessary to prevent adverse effects on the Enterprise because of the new policy. This impact analysis will ensure that an implemented policy has its intended effect in the Enterprise.

Once the digital policy is ready to be deployed, The Digital Policy Management Capability shall, through secure configuration management, provision the digital policy for distribution and deployment. This coordinates the operations of a specific policy (e.g., at a certain time, date, and destination or on the occurrence of a specific event) for allocation and execution for changing needs.

After the digital policy has been deployed or prior to error conditions occurring, it is necessary to proactively detect errors and issues with the digital policy. The Capability shall perform policy assessment to ensure that the digital policy is executing as expected and shall assess the effectiveness of the digital policy after every authorized change. Digital Policy Management shall rely on Enterprise Audit and Monitoring to determine whether it is time to make a change based on indicators that are received by the Organization. Policies shall be defined by authoritative sources, and a means for identifying the source of references shall be established within the Enterprise.

The Digital Policy Management Capability shall store the root source of a digital policy, which points to authoritative sources. Digital policies shall be stored by the Configuration Management Capability. The Configuration Management Capability shall also be responsible for the deployment of digital policies to the applicable devices throughout the Enterprise. The Capability shall be able to deprecate (still active but use is discouraged) legacy policies to ensure that they are accessible.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The Organization has defined the overarching policies, which are verified, validated, and provided by an authoritative source(s).
2. The Enterprise provides the necessary protections to prevent the loss or compromise of digital policies.
3. Endpoints (a service connection to where a network begins or ends) where the policy is executed are configurable.
4. The endpoints are responsible for enforcing the policies.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability allows for creation and deprecation of policies.
2. The Capability provides assessment procedures to make sure policies are effective.
3. The Capability ensures generated policies are associated with an authoritative source that can be verified.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

The Organization will ensure that a documented system exists and is implemented for managing the machine-readable policies that are used to enforce how resources are managed, used, and protected. More specifically, the Digital Policy Management Capability dictates and oversees how digital policies are generated, converted, deconflicted, validated, assessed for effectiveness, provided for distribution, and executed. The Organization will store policies in a centralized manner, and each resource will be assigned a set of policies applicable to its mission, tasks, and the entities that use it.

The Organization addresses the challenge of multiple sources of sometimes conflicting policies and the task of settling on a cohesive set of policies to operate within an Enterprise. Organizations will define policies at a central location through authoritative sources within the Enterprise. If there are conflicting policies, the Organization will make the decision to choose the correct policy for implementation based on specified decision factors, such as written policy or mission needs. The Enterprise will employ digital policy-based authorization and access enforcement when required to protect mission resources in a dynamically changing environment.

The Organization will employ business rules and doctrines for conversion between non-digital policies and digital policies that can be tested to ensure they meet a cohesive policy to be carried out on the Enterprise. The Enterprise will employ established and defined digital policies at a central location by creating a policy hierarchy that allows the translation of policies into a common formal language. This will determine any conflicts and inconsistencies between the new policy and other policies (either active or awaiting activation). An administrator in the Organization will analyze adverse impacts associated with a conflicting policy.

An administrator within the Organization will manually assess whether a digital policy is in compliance with top-level policies before the policy is implemented. The Organization will approve and distribute the policy to Configuration Management for final translation into machine-executable code. This will enable policies across an Enterprise in a uniform manner; distribution will occur from a central authority from within the Enterprise (see Configuration Management). The Digital Policy Management Capability will be able to query the Configuration Management Capability to determine the status of policy implementations, especially to determine the cause of failure of a deployed policy.

The Organization will provide a mechanism for regular digital policy audits to review all policies in use on a network and will ensure that they are necessary and fulfilling their original purpose. Over time, missions and usage of systems change. If they are not audited, digital policies can become redundant or noncompliant, which can cause systems to become vulnerable. These policy audits identify any unnecessary policies, policy redundancies, and where an up-to-date policy is needed. After an automated and/or manual assessment phase, the enforcement point of a policy renders a decision; it audits that decision and pushes that event into the Enterprise Audit Management function to be assessed. An administrator will conduct the local implementation. When the Capability becomes available globally, it will be used at the Enterprise level to make necessary adjustments to the digital policies based on the audit findings (see Enterprise Audit Management Capability).

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- System Protection–The Digital Policy Management Capability relies on the System Protection Capability to enforce digital policies.
- Configuration Management–The Digital Policy Management Capability relies on Configuration Management to distribute digital policies and address final translation to devices on the network.
- Attribute Management–The Digital Policy Management Capability relies on the Attribute Management Capability to provide attributes associated with an entity or resource, which are used to determine applicability of digital policy.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Digital Policy Management Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Digital Policy Management Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Digital Policy Management Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Digital Policy Management Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Digital Policy Management Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Understand Mission Flows–The Digital Policy Management Capability relies on the Understand Mission Flows Capability to provide information about mission flows within the Enterprise.
- Understand Data Flows–The Digital Policy Management Capability relies on the Understand Data Flows Capability to provide information about data flows within the Enterprise.
- Communication Protection–The Digital Policy Management Capability relies on the Communication Protection Capability to provide the secure medium by which digital policies are distributed.
- Data Protection–The Digital Policy Management Capability relies on the Data Protection Capability to provide protection mechanisms for digital policies.

- Risk Mitigation–The Digital Policy Management Capability relies on the Risk Mitigation Capability for information used to mitigate Enterprise risks by creating, changing, or deleting digital policies.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AC-2 *ACCOUNT MANAGEMENT*	Control: The organization manages information system accounts, including: b. Establishing conditions for group membership; Enhancement/s (7) The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles.
AC-4 *INFORMATION FLOW ENFORCEMENT*	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. Enhancement/s: (10) The information system provides the capability for a privileged administrator to enable/disable [Assignment: organization-defined security policy filters]. (1) The information system provides the capability for a privileged administrator to configure [Assignment: organization-defined security policy filters] to support different security policies. (4) The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [Assignment: organization-defined information security policy requirements].
AC-6 *LEAST*	Control: The organization employs the concept of least privilege,

PRIVILEGE	allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Enhancement/s: (1) The organization explicitly authorizes access to [Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information]. (2) The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions. (3) The organization authorizes network access to [Assignment: organization-defined privileged commands] only for compelling operational needs and documents the rationale for such access in the security plan for the information system.
AC-14 *PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION*	Control: The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Enhancement/s: (1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/ business objectives.
AC-19 *ACCESS CONTROL FOR MOBILE DEVICES*	Control: The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; Enhancement/s: (1) The organization restricts the use of writable, removable media in organizational information systems.

	(2) The organization prohibits the use of personally owned, removable media in organizational information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner. (4) The organization: (a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s).
AU-9 *PROTECTION OF AUDIT INFORMATION*	Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. Enhancement/s: (4) The organization: (a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and (b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.
CM-5 *ACCESS RESTRICTIONS FOR CHANGE*	Control: The organization defines documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.
IA-2 *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)*	Enhancement/s: (5) The organization: (a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and (b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.
MA-4 *NON-LOCAL MAINTENANCE*	Control: The organization: Enhancement/s: (4) The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either: (a) Physically separated communications paths; or (b) Logically separated communications paths based upon encryption. (5) The organization requires that: (b) A designated organizational official with specific information

	security/information system knowledge approves the non-local maintenance. (7) The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Digital Policy Management Directives and Policies

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
IC Information Sharing Strategy, 22 February 2008, Unclassified	Summary: This document lays out a strategy for better information sharing and providing more effective communication between the participants in the national security community that improves the quality, applicability, and usage of the results of the intelligence process.
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance,	Summary: This guidance outlines a common framework for Identity, Credential, and Access Management (ICAM) within the Federal Government and provides supporting implementation guidance for program managers, leadership, and stakeholders planning to execute a segment

Version 1.0, 10 November 2009, Unclassified	architecture for ICAM management programs. It includes courses of action, planning considerations, and technical solution information across multiple federal programs spanning the disciplines of ICAM. Federal Identity, Credential, and Access Management (FICAM) mentions three core support areas that enable successful access management for both physical and logical access: Resource Management, Privilege Management, and Policy Management.
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Digital Policy Management Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	

Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation–Locally versus globally implemented solutions will affect the solution’s performance and how well it will scale. In addition, the number and variety of endpoints will affect the complexity of managing digital policies.
2. Manpower to implement, maintain, and execute–Designing unique policies will require the efforts of dedicated personnel (i.e., policy engineers).
3. Storage requirements–This Capability provides a repository for digital policies.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the [capability name] Capability.

- The Enterprise shall provide for the management of digital policies, which consists of a set of functions used to generate, convert, deconflict, validate, assess effectiveness, provision for distribution and deployment, and execute machine-readable policies used to enforce how resources are managed, used, and protected. These policies may include rules for authentication (e.g., trusted authorities, criteria for determining authenticity), system configurations, access rules, authorized sources of record or sources of reference, transport connectivity, bandwidth allocation and priority, audit event collection, and computer network defense monitoring and response (e.g., course of action).
- The digital policy management system shall be able to generate and manage globally and locally applicable policies.
- The digital policy management system shall be able to respond rapidly to changing conditions and to new mission requirements.
- The digital policy management system shall be able to scale to accommodate the global scope of a federated Enterprise.
- The digital policy management system shall be able to operate effectively in both strategic and tactical environments.
- The digital policy management system shall be flexible enough to adjust policies in real-time (or as close to real-time as possible) to respond to changing needs.
- The digital policy management system shall convert policies into various formats, as necessary, to be readable to the applicable devices and systems. Conversions shall be automated, where possible.
- The digital policy management system shall include deconfliction to determine whether policies are consistent and contain no internal contradictions within the policies or between policies.
- The digital policy management system administrator shall manually decide the correct policy/policy statement to follow to implement in the Enterprise.
- The digital policy management system shall perform policy assessment to ensure that the digital policy is executing as expected and has its intended effect in the Enterprise.

- The digital policy management system shall assess the effectiveness of the digital policy after every authorized change.
- The digital policy management system shall use an Enterprise secure configuration management system to provision digital policies for distribution and deployment.
- Policies shall be defined by authoritative sources, and a means to identify the source of references shall be established within the Enterprise.
- The digital policy management system shall store the root source of all digital policies, which point to authoritative sources.
- The Enterprise shall be able to deprecate (still active but use is discouraged) policies that are kept in a policy store to ensure these policies are accessible.